Introduction

E-commerce environment

The typical network administrator must support many different products in his networked environment. This is particularly true when it comes to applications that perform e-commerce transactions. Products that perform e-commerce transactions typically have their own administrative controls, if they have any administrative controls at all. The availability of an add-on policy system that could monitor e-commerce transactions and enforce policy simultaneously for multiple products would provide significant value. This invention addresses that need by describing a means of interposing new policy components between existing system components. The step of interposing the new policy component requires knowing the interface specification between the components at the point of insertion.

Although not there yet, the industry is currently driving towards the adoption of publicly available standards for the interaction between the major software components involved in e-commerce transactions. The trend in the industry now and in the expected future is for software vendors to provide system components that must work together. Publicly available standards are believed to be the best way to achieve reliable and proper inter-operation between components provided by different vendors. The availability of publicly available standards will increase the value of this invention, however, all that is necessary for implementing this invention is access to the interface specification, however obtained. In order to demonstrate the principles behind the invention we concentrate on a typical configuration used by e-commerce applications. The implementation does not depend on the number, or detailed nature of the components.

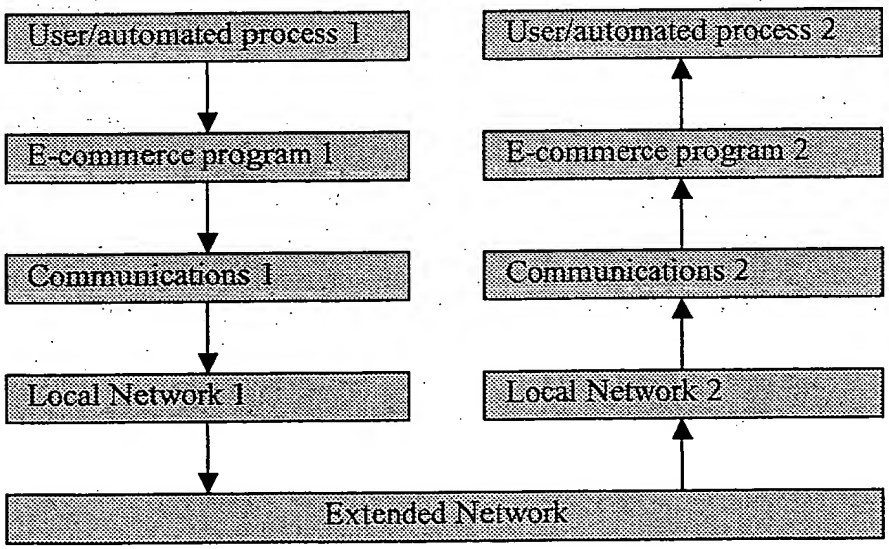

Figure 1 illustrates a likely sequence of interactions between software components used to carry out an e-commerce transaction.

Exhibit C

A typical e-commerce transaction might involve the sequence of software components diagrammed in figure 1. The top left box in the stack labeled **User/automated process 1** represents a person or computer program that is specifying the nature of an e-commerce transaction. Specifying the nature of the transaction could be accomplished by anything from selecting options in a user interface to programming an automated agent to exercise a programmatic interface. **E-commerce program 1** processes this information and places it into a known form. A known form contains data encoded according to a specification such that other programs capable of applying the specification to the known form can meaningfully process the data. There may be more than one specification available and therefore more than one known form used by the e-commerce program. **E-commerce program 1** transfers this information to

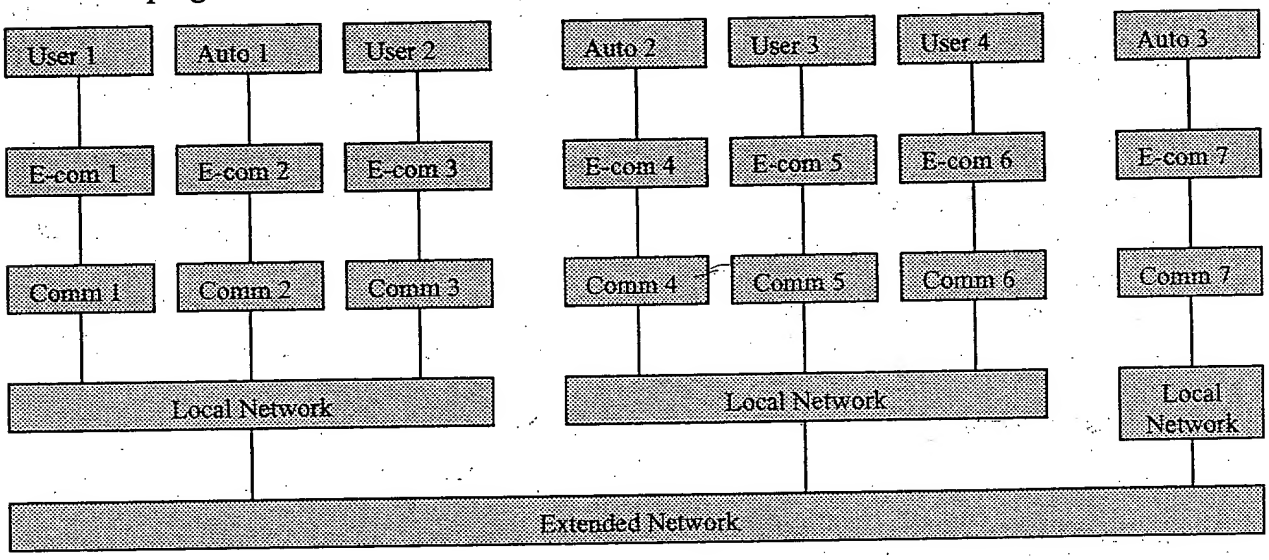

Figure 2 illustrates a network of several complete e-commerce capable installations thereby providing a more realistic model of the real world.

communications system 1 which in turn sends the information to the communications interface of another e-commerce program. The communications may pass through a local network and then over a more extended network such as the Internet. The information may be transformed several times in transit. The details of how the known form is delivered to the **Communications system 2** are not important for this example. **Communications system 2** delivers the known form to **E-commerce program 2**, which ultimately interprets the known form. In practice, the activity illustrated in this diagram is repeated many times over, where the e-commerce programs could be provided by many different vendors and be deployed in many different locations. Furthermore, transactions could potentially flow either direction. Figure 2 illustrates a more realistic model for the current e-commerce environment.

Figure 2 shows a configuration composed of four distinct users (**User 1** through **User 4**) and three automated e-commerce processes (**Auto 1** through **Auto 3**). An example of an automated process would be an e-commerce store that supports electronic purchasing. In the example shown in Figure 2 each e-commerce stack employs different e-commerce programs that may have each been written by a different vendor. For the purpose of illustration, each communications system (**Comm. 1** through **Comm. 7**) is assumed to be different from the other communications system. Assuming both **User 1**

and **User 2** employ graphical user interfaces to interact with **E-comm 1** and **E-comm 3** respectively there is no reason to expect that the user interfaces will be the same or even similar. Analogously, if **Auto 1** and **Auto 2** are interacting with **E-comm 2** and **E-comm 4** programmatically, there is no reason to expect the programmatic interfaces to be the same or similar. However, under the conditions specified at the beginning of this document, all of the e-commerce programs produce one of the known forms that can be processed by any other e-commerce program that supports the same specification.

E-commerce filters

This invention involves interposing new software components between one or more of the software components shown in the above figures. These new software components would only be interposed where the data is cast in a known form that enables the interposed software to interpret all or some of the characteristics of the e-commerce transaction flowing through it. For illustrative purposes, Figure 3 indicates some of the positions (with diamond shapes ◇) where new components could meaningfully be interposed based on the scenarios used to develop the earlier figures.

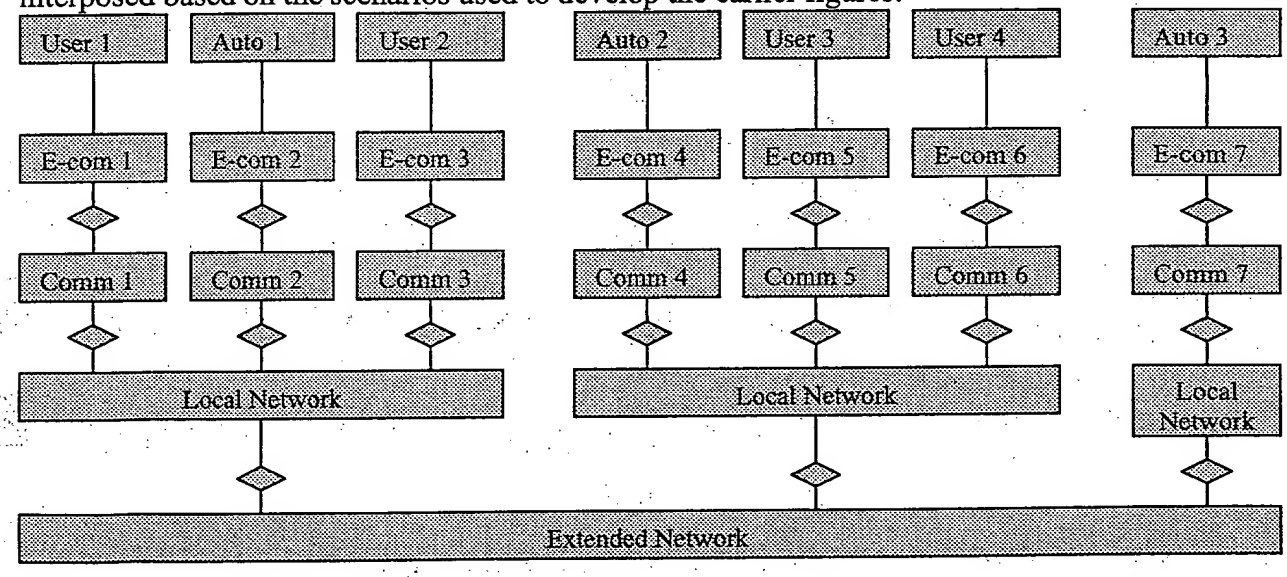

Figure 3 shows potential locations for interposing software components that analyze e-commerce information, possibly taking action based on the processing results. The diamond shapes (◇) represent new software component called a filter that is interposed between software components that process e-commerce transaction information.

The interposed software components (hereinafter referred to generically as "filters") have the potential to analyze the e-commerce traffic passing through them and possibly take action based on the results of the analysis. In spite of the fact that the filters appear at different levels of the communications hierarchy, they have the potential for extracting equivalent information. For example, a filter interposed between **E-com 1** and **Comm 1** could (in this example) do the same analysis as a filter interposed between **Comm 1** and the **Local Network**. Although any analysis of the e-commerce transactions could be performed, this invention anticipates those analysis will fall into two categories, analysis for the purpose of collecting information across some administrative domain and analysis pursuant to enforcing a policy for some administrative domain. The

administrative domain could be a single machine, a single user who could appear on different machines, a collection of users or machines or any combination thereof.

Policy administration

In the currently available environment, policy and the collection of e-commerce

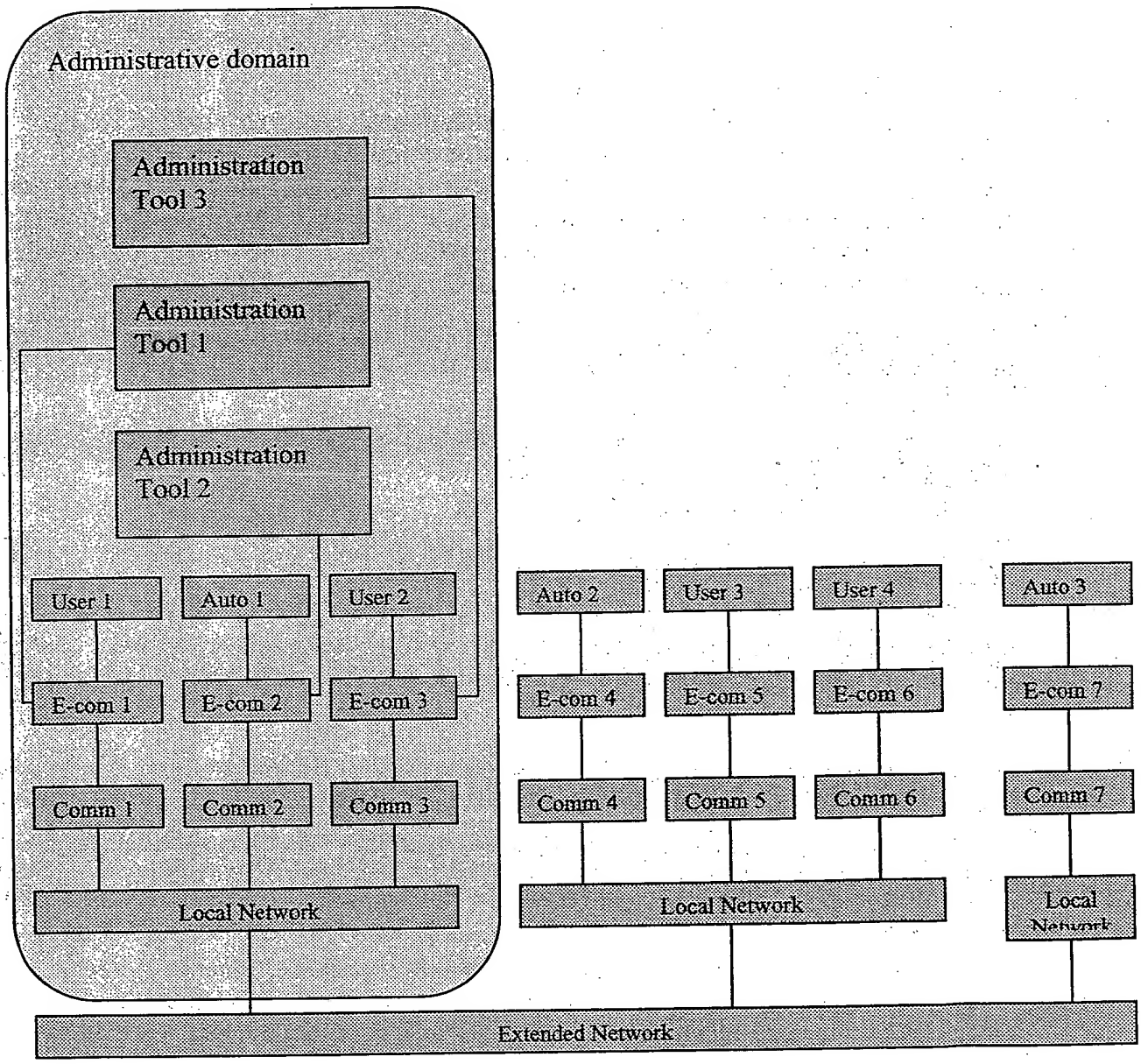

Figure 4. Multiple administration programs are typically needed to set policy for and collect information from e-commerce programs provided by different vendors.

transaction information may be enabled within either the User/automated process components or the e-commerce program. In order to collect equivalent data or enforce uniform policies across an administrative domain, one would need to either find a single

administrative program that can provide the equivalent administrative capabilities for software from three different vendors, or perform administrative functions with three different administration programs for the three different products. The later case is more likely and is illustrated in figure 4.

Consider the case where administrative capabilities do exist in the user/automated process components or the e-commerce programs. In a multi-product environment, those capabilities can only provide consistent coverage across an administrative domain when each product supports similar administrative capabilities. In the general case, in which the administrative domain contains different products (perhaps from different vendors), administrative capabilities will be specific to each product or vendor and will not enable

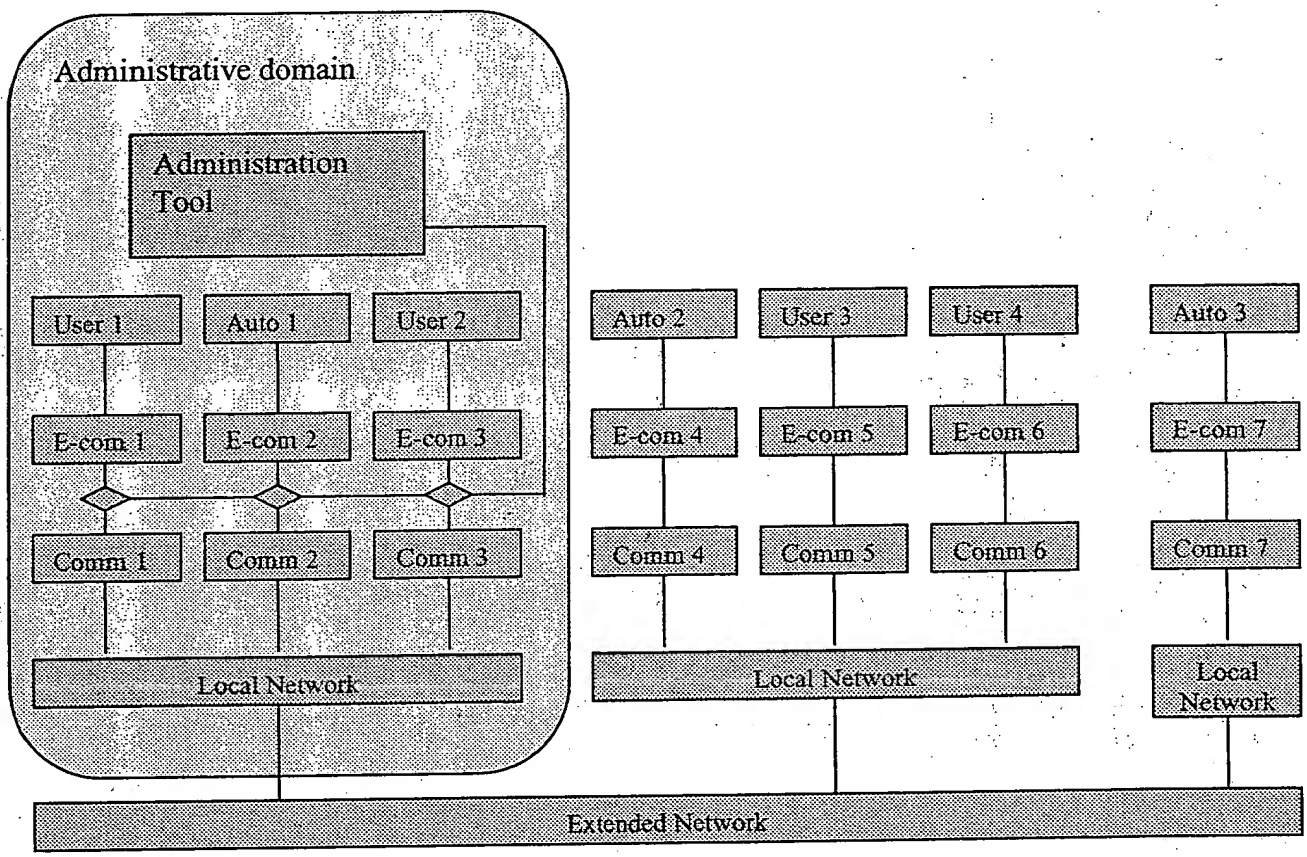

Figure 5. A e-commerce based filter controlled by an administration program is interposed uniformly across an administrative domain at the interface between the e-commerce program and the communications system.

uniform capabilities across the domain. Of course, even if similar administrative capabilities are available from all products, it may not be practical to apply a uniform policy across all of the e-commerce programs. For instance, the desired policy may be to enforce limits for certain operations within the administrative domain (e.g. the total amount of money spent). In the scenario illustrated in figure 4, this would be difficult or impractical since the administrative programs do not share information between them so no single program gets an overall view of the administrative domain.

In this invention we approach providing comprehensive and uniform coverage across an administrative domain by adding a e-commerce based filter (as illustrated in

Figure 3) across a layer of the e-commerce based e-commerce stack. One possible implementation of this concept is illustrated in figure 5.

The known form of the information allows it to be analyzed independent of the particular e-commerce program from which it originated. In cases where e-commerce transaction information is being collected, the information can be accumulated based on the known form of the e-commerce transaction data and therefore traffic originating from different e-commerce programs can be combined. Similarly, enforcement of policies specifiable at the e-commerce transaction level can be evaluated seamlessly across e-

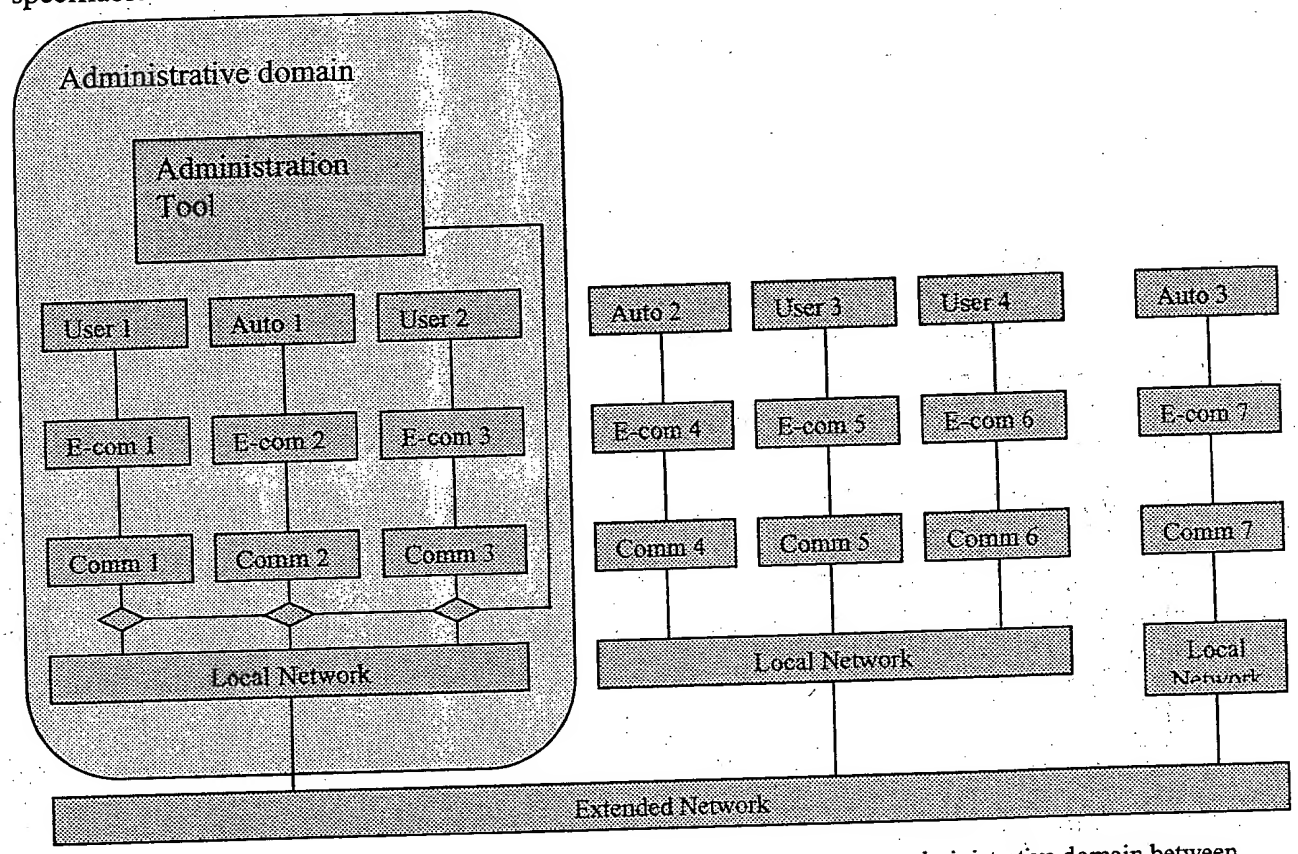

Figure 6. A e-commerce based filter may also be interposed uniformly across an administrative domain between the communications system and the local network.

commerce products, even if they come from different vendors. Figure 5 illustrates but one possible configuration for using e-commerce based filters uniformly across a heterogeneous administrative domain. Figure 6 illustrates another configuration in which e-commerce based based filtering could potentially be accomplished. As anticipated by figure 3, e-commerce based based filtering could also be carried out at the interface with the extended network as is illustrated in Figure 7.

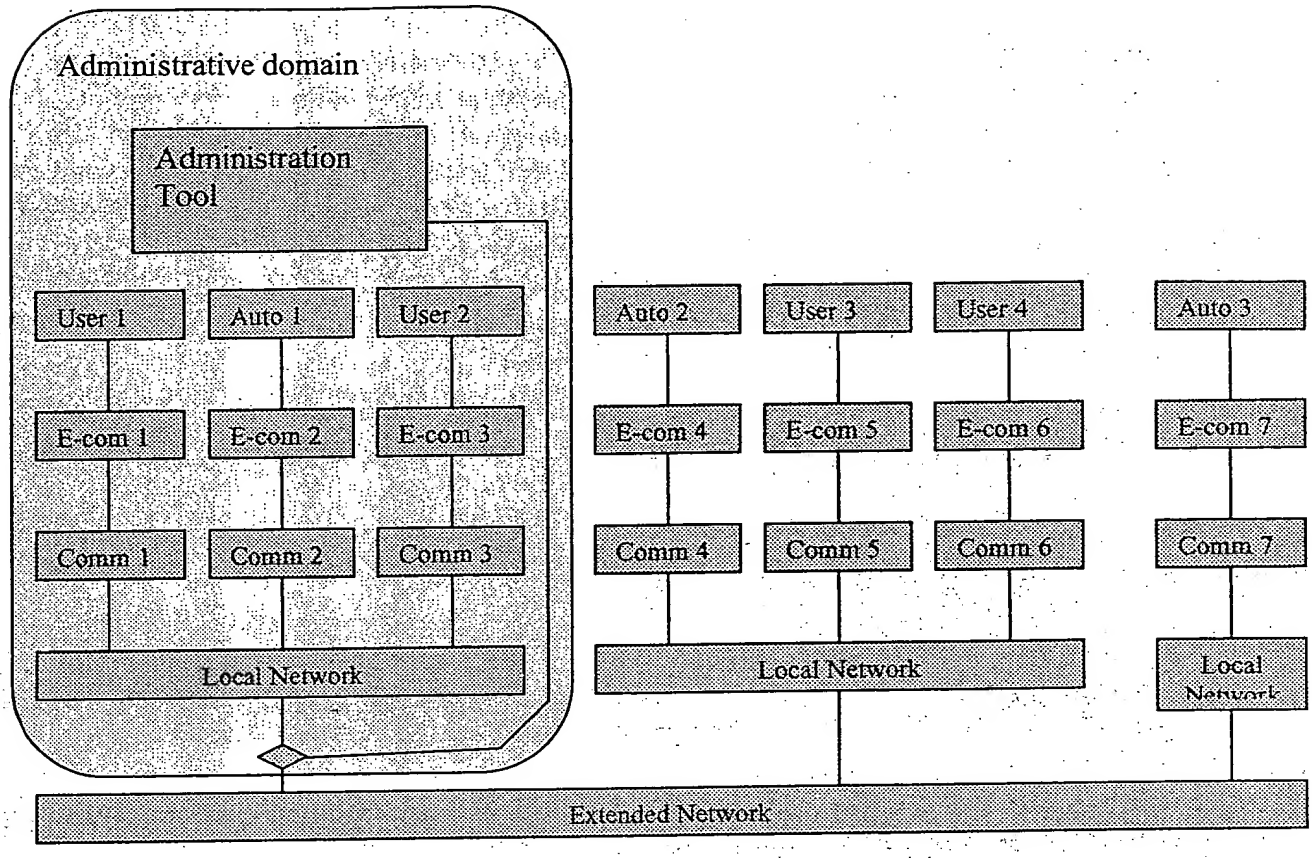

Figure 7. A e-commerce based filter may also be interposed uniformly across an administrative domain between the local network and the extended network.

The impact of cryptographic technologies

Cryptographic technologies are widely employed in e-commerce transactions for identifying the source of messages, verifying their authenticity and hiding their content from unauthorized people or programs. In some system configurations, cryptographic technologies will limit the ability of filters to analyze or modify data in the known form. However, there are many system configurations that provide cryptographic protections without preventing the proper operation of filters. Using the same illustrative architecture as in figures 2 through 7, figure 8 illustrates a popular system configuration in which cryptographic techniques are used to provide a secure private tunnel through an insecure public network. In this case, the filter shown in figure 8 would not be limited by the encryption used to construct the secure private tunnel.

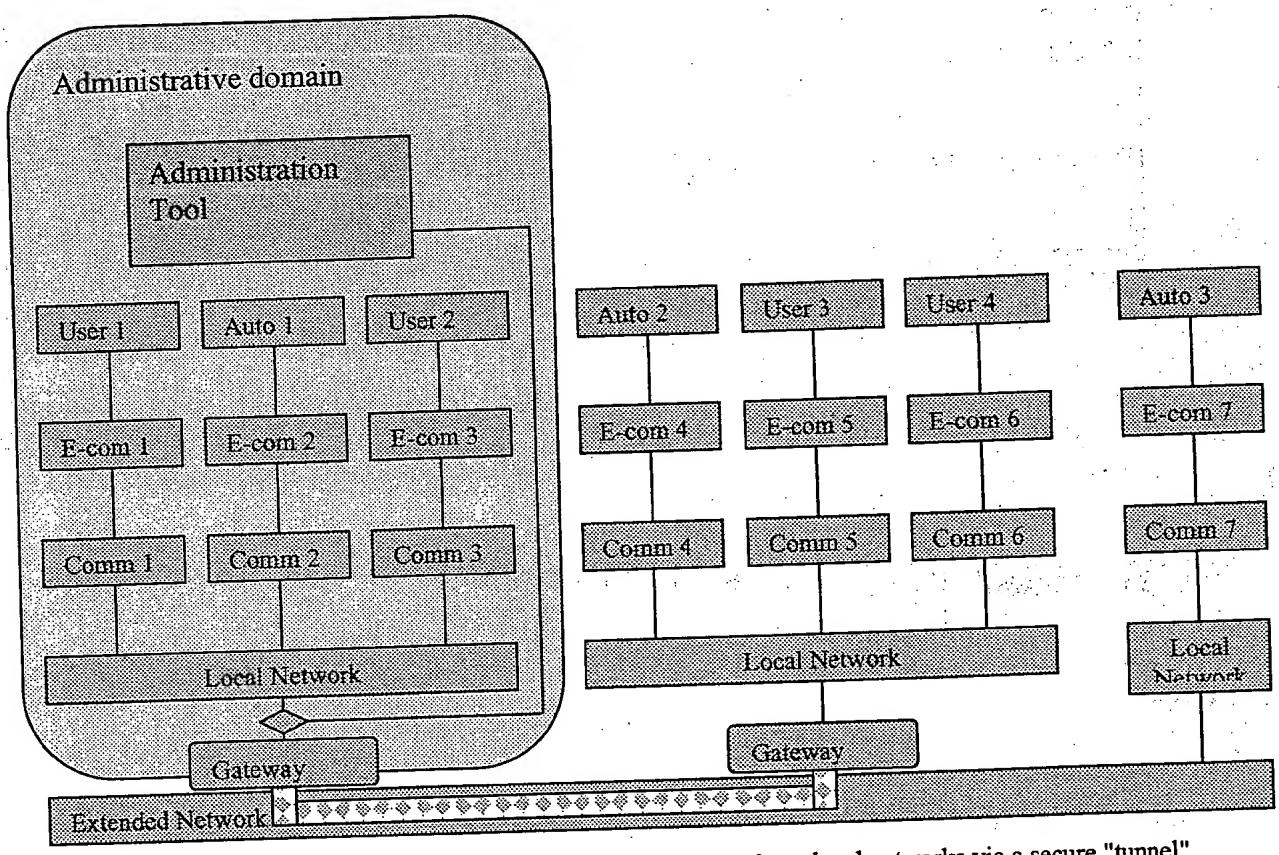

Figure 8 Cryptographic technologies may be used to connect two private local networks via a secure "tunnel" through a public network, illustrated here by a shaded pipe. This does not interfere with an e-commerce based filter interposed between the local network and the extended network (or indeed at any higher layer).

In the systems where data encryption is introduced in the communications component, a filter located at a gateway (as shown in figure 8) may not be able to meaningfully process the known form. In order to meaningfully process encrypted data, the filter would require access to the decryption key, which is contrary to most security policies. This situation is illustrated in figure 9. One way of avoiding the situation illustrated in figure 9 is to position filters at the e-commerce program / communications component boundary as is illustrated in figure 10. The configuration illustrated in figure 10 has the advantage of working seamlessly with many forms of session layer

cryptography, such as Secure Sockets Layer (SSL) services. SSL is a popular method for

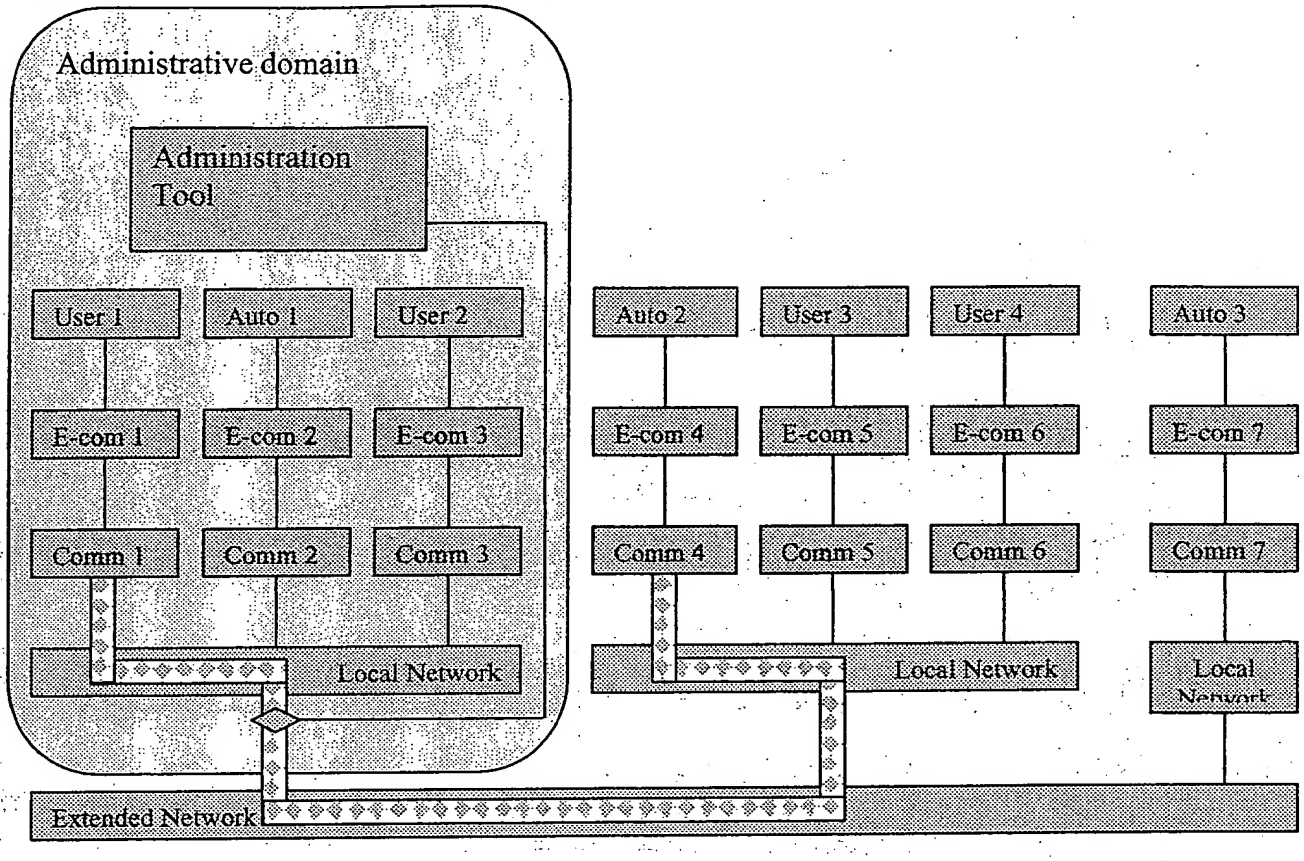

Figure 9 shows the path of encrypted data when the encryption is performed within the communications layer. Note: the filter component illustrated in this figure could be moved higher in the stack (as in figure 10), or the filter could be given access to the decryption key.

including encryption and authentication into e-commerce systems.

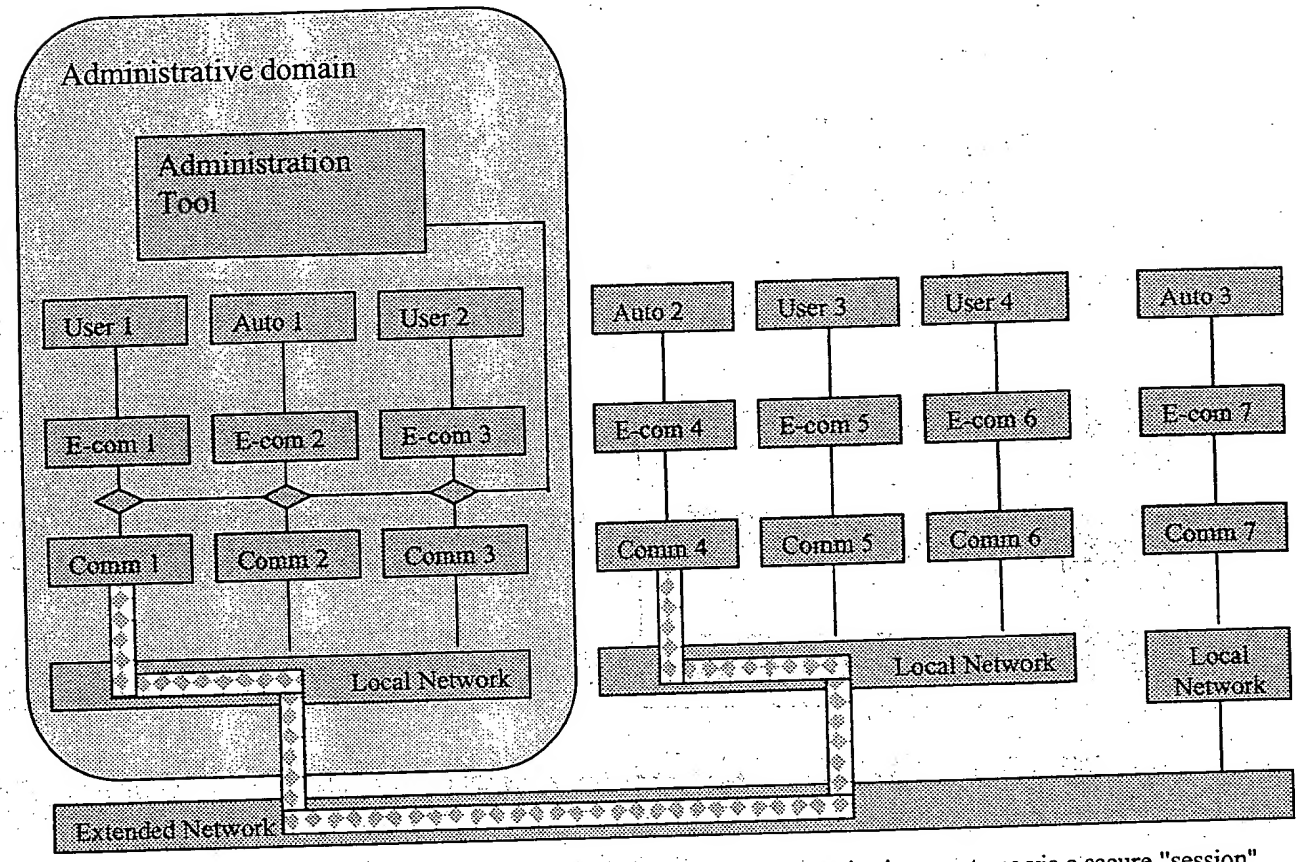

Figure 10. When cryptographic technology is used to connect two communications systems via a secure "session", it does not interfere with a e-commerce based filter interposed between the e-commerce programs and the communications systems.

Filtering in the presence of cryptography

Cryptographic technologies are already widely used with e-commerce transactions, and this trend is expected to continue as the industry grows. Therefore, e-commerce based filters will have to operate in the presence of cryptography.

E-commerce transactions may flow through a wide variety of cryptographic technologies, so e-commerce based filters need a variety of strategies for operating in their presence. Such strategies include but are not limited to the following:

- The e-commerce based filter may be interposed above the components that implement the cryptographic technology. Figure 8 and Figure 10 illustrate this strategy, which is appropriate when the administrator has some flexibility in choosing where to interpose the filter.

- The e-commerce based filter may be given the keys necessary to encrypt and decrypt the messages flowing through it. Figure 9 illustrates this strategy, which is appropriate when the filter has access to the key(s) necessary to decrypt the data.

- A e-commerce based filter may include two cryptographic proxies, paired with the communications programs at each end of a secure "session". Each proxy connects to one of the communications programs and plays the role of the other communications program in the cryptographic protocols they use, thus forming two separate secure "sessions" with the filter logic between them. Figure 11

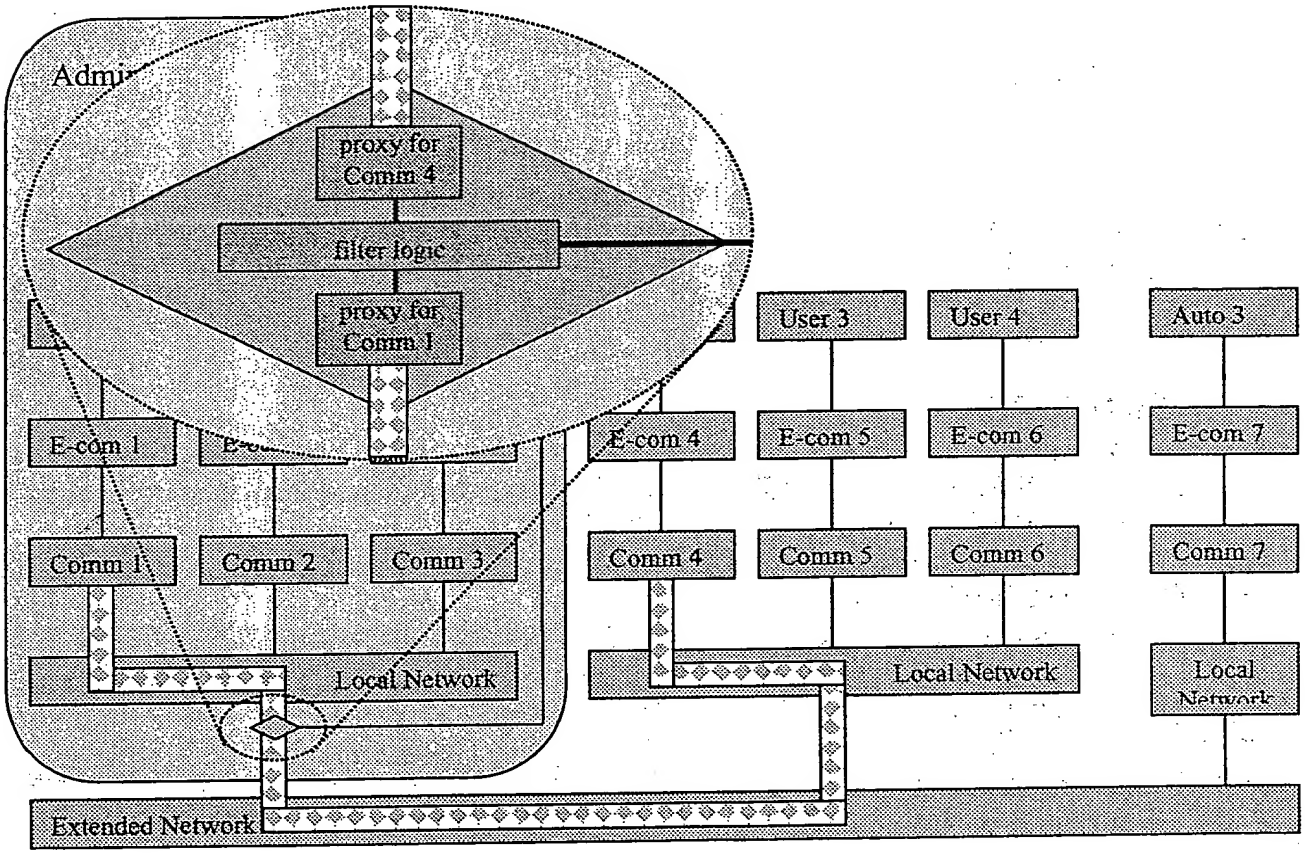

Figure 11. When cryptographic technology is used to connect two communications systems via a secure "session", it does not interfere with a e-commerce based filter that includes cryptographic proxies.

illustrates this strategy, which is appropriate when asymmetric-key (also known as public-key) cryptographic technologies are used.

- A e-commerce based filter may be given a key that can be used to decrypt only part of the message as when the communications are encrypted with multiple keys, where one of the keys is provided to the filter. Figure 9 illustrates this strategy.

Filter capabilities

Filters can be programmed to reconstruct transactions even if the transaction is broken up into multiple pieces. This can be accomplished by providing persistent storage in the filter that associates the appropriate pieces in order to build a complete picture of the transaction. Using such technology, filters can potentially know the transaction parties, timings, and specific details such as quantities and part numbers. It will also be

possible in some cases for the transactions to be modified by the filters so as to create new functionality in the system or enforce specific policies from within the filters.

Business related capabilities

There are four fundamental classes of activity that are enabled by the invention:

1. Rerouting transactions
    a. Automated bundling
    b. Offer transaction to third party
2. Modifying transactions
    a. Blocking transactions
    b. Stalling transactions
    c. Alerting on selected transactions or situations
3. Recording transactions
4. Generating new transactions
    a. Ordering related goods
    b. Ordering related services

Business models

- Immune system model: Collect information from subscribers in a way that appropriately protects the customer's privacy. Centrally analyze the data in order to detect unacceptable transactions and then in response, possibly in real time, distribute identification information to subscribers filters that can block or stall detected transactions.
- Build a security team that is responsible for staying current on the late breaking Internet-based scams. The security team would learn how to identify the scam by analyzing the transactions that are used to carry out the scam. The identification technology could be supplied to subscribers as updates to their filters. When a filter running at a customer sited identified a scam related transaction the security company could provide value added services such as obtaining legally relevant information for future prosecution.
- A third party transaction recording company. The transaction record repository company installs filters across a subscriber's organization in order to collect a record of the transactions undertaken by the organization. These filters encrypt the transaction information and send it to the third party repository. The repository time stamps the transaction history and archives it for a period of time. The repository company would not be able to interpret the encrypted data.
    - The subscriber company could encrypt with a public/private key pair (a,b) and could then throw away the private key(a) (or claim to have thrown it away when in court). Then no-one would be able to decrypt the data in the repository, however, if the subscriber wanted to legally prove that a particular transaction took place at or before the repository time stamp, they could recover the data from their own archive, encrypt the data with the public key (b) and show that it matched the encrypted data in the archive. This solves the often-mentioned problem with having a third party hold your business data. When a government entity attempts to get at archived data held by a third party the typical response of the third party is

to immediately turn over the data, whereas, when companies are asked to turn over their data, they typically find a way to either not comply or partially comply in a way that will protect their information.
    - The subscriber company could encrypt with a symmetric key and hold the key so only the holder of the key would be able to decrypt the data in the archive.
- Sell filter based heuristics for detecting potential e-commerce scams as a subscription service. The power of filter-based heuristics would be greater than heuristics implemented within a single product since they would have information from an entire administrative domain to analyze.
- Sell a subscription service that keep up with changing export laws, tax laws etc. and provides these as intelligence in filters that monitor/enforce compliance.
- A third party vendor provides filters to a customer. After installing the filters, the customer would search for the best deal they could find and then execute a purchase transaction. The filter would intercept the purchase transaction and offer the third party vendor the opportunity to supply the product or service at the discovered price. The third party vendors could then re-direct the order to themselves. There could be a variety of incentives provided to the customer by the third party vendor in order to obtain the business, such as an overall discount provided to the company at the end of the year based on the total amount of business transacted.
- A service that audited the filter policies and certified them as in compliance with some standard, consistent with best practices etc.
- Subscription service that provides additional security checks before a transaction can be completed. For instance, extend the certification/authentication function commonly present in e-commerce applications to include enforcing additional policy relative to signatures; e.g., that a person is authorized to sign in a specific role (purchaser, co-signer) or cross-checking information held at different sites; e.g., multiple banks may have to assure payment when the funds covering a transaction are spread across different accounts.

Some claims that occurred to us; not all the text is covered by these claims

(1) A subsystem interposed between two or more parties that intercepts e-commerce transactions and takes actions based upon the properties of the e-commerce transaction; where the presence of the subsystem does not require any changes to the protocols used by the parties.

(2) A system as in claim (1) where the subsystem interposed between two or more parties includes one or more software components that identifies e-commerce transaction related traffic even when other traffic is passing between the parties.

(3) A system as in claim (1) where the subsystem interposed between two or more parties includes one or more software components that deduces what if any action should be taken in connection with an e-commerce transaction arriving at the subsystem.

    a. A system as in claim (3) where the action is deduced in part or whole by applying predefined rules to the contents of one or more messages that comprise an e-commerce transaction.

b. A system as in claim (3) where the action is deduced in part or whole by applying predefined rules independent of the contents of any messages that comprise an e-commerce transaction.
c. A system as in claim (3) where the action is deduced by applying predefined rules based entirely on the origin or destination of one or more messages that comprise an e-commerce transaction.
d. A system as in claim (3) where the action is deduced by supplying another software subsystem information and receiving a reply.
e. A system as in claim (3) where the action is deduced by interacting with a human

(4) A system as in claim (1) where the subsystem interposed between two or more parties includes one or more software components that modifies e-commerce transactions arriving at the subsystem before it is passed to the intended party.

(5) A system as in claim (1) where the subsystem interposed between two or more parties includes one or more software components that does not pass a received message to the intended party.

(6) A system as in claim (1) where the subsystem interposed between two or more parties includes one or more software components that pass a received message to a different party than the intended party.

(7) A system as in claim (1) where the subsystem interposed between two or more parties includes one or more software components that pass a received and modified message to a different party than the intended party.

(8) A system as in claim (1) where interposed is interpreted to mean that the subsystem is comprised in part or entirely of a software layer inserted between two existing software layers such that the pre-existing software layers continue to operate properly in the event the subsystem takes no action.

(9) A system as in claim (1) where interposed is interpreted to mean that the subsystem is comprised in part or entirely of a software object inserted between two existing software objects such that the pre-existing software objects continue to operate properly in the event the subsystem takes no action.

(10) A system as in claim (1) where interposed is interpreted to mean that the subsystem is comprised in part or entirely of a software component inserted between two existing software components such that the pre-existing software components continue to operate properly in the event the subsystem takes no action.

(11) A system as in claim (1) where parties is interpreted to mean any software that represents a person or institution that has the ability to transfer goods, services or money.

(12) A system as in claim (1) where parties is interpreted to mean any software that represents a person or institution that has the ability to transfer goods, services or money.

(13) A system as in claim (1) where *e-commerce transaction* is interpreted to mean any message traveling between any of the parties related to the transfer of goods, services or money.

(14) A system as in claim (1) where *e-commerce transaction* is interpreted to mean any collection of messages traveling between any of the parties that together enable the transfer of goods, services of money.